Published and Copyright (c) 1999 - 2008
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1143 10/23/09

~ Fake Security Software ~ People Are Talking! ~ Swine Flu Scams!
~ Cybercrime Gets Worse! ~ New Macs for Holidays! ~ Win 7 Launched!
~ New Bait for Phishers! ~ Nigeria Fights Crime? ~ China Ready for War?

~ Craiglist Suit Dumped! ~ Snow Leopard on a PC? ~ Borderlands Out!

-* Lobbying for Net Neutrality! *-
-* Microsoft Opens First Retail Store! *-
-* Man Suspected of Encouraging Suicides Online *-

=~=~=~=

->From the Editor's Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""

Well. the "party" is over - not that there really were any. But, you just know that the talk has to be big while the "cat" is away! But, it's good to have the family united once again - we all missed my wife, and glad that she's back! I guess it's true that you really never appreciate something (or in this case, someone) until it's (she's) gone! Anyway, everything is back to normal once again!

Lots of interesting stories in this week's issue. Windows 7 has been released. Net Neutrality gets support and a fight against the proposals. New (or re-vamped) Macs due shortly. Swine flu scams abound on the web! And lots, lots more! It's been a good week for technology news, for a change.

So, while I rest up and try to shake off some cold symptoms (I hate being sick, or even close to being sick!), let's move right along and get into the meat of the issue!

Until next time...

=~=~=~=

PEOPLE ARE TALKING
compiled by Joe Mirando
joe@atarinews.org

Hidi ho friends and neighbors. Yeah, you guessed it... there aren't enough messages in the NewsGroup to put together a good column. So instead, I'm going to talk about a couple of things... yeah, politics and... politics. [grin]

First of all, let me talk a little bit about this year's Nobel Peace Prize. Yeah, Dana was right. IF I'd been up to it two weeks ago, I would have had something to say about it. I've heard a lot of noise in the past two weeks about whether or not President Obama 'deserves' the Nobel Prize... like it's a matter open to debate. The fact is that the Nobel Committee decides. It's not open for debate, it's not a call-in reality show where one contestant gets voted off each week. There are people who specifically invited to submit the names of candidates for the prize. The

’nominators’ are people recognized by the selection committee as having some expertise.... various government officials and politicians, historians, former Peace Prize winners, former advisers to the Nobel Institute, etc. Not what you’d call a stacked deck, by any means.

After that, the list is narrowed by the Nobel Committee, and the resulting ’short list’ is given to the advisers to the Nobel Institute, who try to arrive at a unanimous decision (and usually, but not always, do).

As you can see, this is NOT a popularity contest.

So why have so many people taken the opinion that it is? Well, first of all, they don’t know what they’re talking about. That usually removes a lot of the annoying obstacles from their path. The idea of the deck being stacked against them gets them all hot and sweaty, and it’s much easier to imagine a vast, inter-continental conspiracy against you rather than just coming to terms with the idea that my might be wrong. Add to that the fact that there’s "no money" in being wrong, either on the radio or on television, and you have the makings for your own special corner of reality where it really doesn’t matter what the truth is as long as you can spout your venom and not have to hear someone tell you you’re wrong. And the fact that you can get a vast majority of the ’pudding-head’ section of the country to listen to and agree with you is the cherry on top.

Now, as far as Obama "not having earned" the prize, how do we decide that? Obviously the Nobel Committee and its advisers disagreed. But what might there criteria have been?

How about... ummm... LEADING. No matter what your political affiliation or your opinion of the president, you cannot deny that the country’s standing in the world is much better now than it was even just a year ago. Is that because of something Obama has actually DONE in the past 10 months? I really don’t think so. Oh, sure, he’s said he wanted to close Gitmo and pull out of Iraq and "finish the job" in Afghanistan, and put huge financial companies on notice for everything from unfair credit card policies to paying bonuses while on the government dole, but none of it has come to fruition yet. And, quite honestly, some of it never will.

But instead of fishing when New Orleans was flooding, instead of sitting there in a classroom reading "Everybody Poops" or whatever he was reading when some sick bastards flew a couple of commercial jets into the World Trade Center, and instead of denying the severity of the economic crisis until even he had to cave in and do something simply to stop the murmuring in the ’audience’ he, whether it was reality or not, was SEEN to be doing something. By the very act of SEEMING to be doing something, he raised the hopes of not only Americans, but of others who want to look to the United States for help, for stability, for a world conscience and had not been able to do that for the previous eight years.

All of a sudden, there was a new sheriff in town... a new wind blowing... an attitude that, just because we had been wrong or less than helpful in the recent past didn’t mean that we could not turn back and rebuild. Because we had made... mistakes... in the past did not mean that we could not admit it and work to fix them. That simply because we had started down one path did not mean that we could not turn around and retrace our steps to bring us back to where ’we’ want to be; that we were not going to simply ignore what needs to be fixed because we’re "in it too deep now".

The announcement of Obama winning the Peace Prize coincided fairly closely

with a world-wide poll about 'trusted countries'.. The United states had jumped by a huge amount over last year. Yet, the country... and the world, for that matter, still teeter on the brink of a financial crisis of almost unimaginable proportions, we're still involved in wars in two countries, and we still have detainees held in Guantanamo Bay. We're still issuing ultimatums to Iran for making nuclear fuel, still putting pressure on our old cold war nemesis, in fact, still doing most of the things that made us wildly unpopular on the world stage.

So why, if so little has changed, do others have more faith in us now than a year ago? I think the answer has a lot to do with perception. For one thing, intelligence tends to be very comforting on the world stage. For another, activity is seen as a good sign. You don't have to solve all the problems, you just have to work on them instead of denying them. And not having a "might makes right" attitude helps too. When that thing happened with the Cambridge professor and the police officer, the White House could have said nothing, it could have sided with the police, or it could have sided with the professor. And, in fact, that's the way it started out... with Obama saying the police acted "stupidly". Remember?

But in its refreshingly introspective style, the new White House amended/changed its opinion and held the now-famous "Beer Summit". But what was REALLY accomplished other than some free advertising for the three brands of beer? It wasn't about the beer. It was about being able to talk. It was about 'sides' getting together and being able to acknowledge one another instead of cutting off all communication. Like my grandfather used to say, "You can be as mad as you want, but ya still gotta talk!" Maybe not about the 'big' problem, maybe not about the actual event. But they were together, face to face, and no one walked away with a bloody nose.

So, yeah, we've got a long way to go. We've got health care issues, security issues, economic issues, immigration issues and probably a dozen more. But we're working on them. Whether or not we ever solve most of them, we're working on them. And THAT'S where progress really begins.

Well, that's it for this time around. Tune in again next week, same time, same station, and be ready to listen to what they are saying when...

PEOPLE ARE TALKING

=~=~=~=

->In This Week's Gaming Section - Video Game Sales Improve Slightly!
"""""""""""""""""""""""""""""""" "Borderlands" Videogame Hits U.S.!
Backyard Football '10!

=~=~=~=

->A-ONE's Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""

Video Game Sales Improve Slightly in September

After six straight months of double-digit declines, U.S. video game sales finally saw an improvement in September.

But the rebound was much more muted than analysts had hoped, a sign that the recession has cut deep into consumer spending on interactive entertainment. Even recent console price cuts weren't enough to push hardware dollar sales higher year-over-year.

Market researcher NPD Group on Monday reported a 1 percent increase in September sales of video game hardware, software and accessories compared with the same month last year. The total came to $1.28 billion. Year-to-date sales were down 13 percent.

Hardware sales dropped 6 percent to $472.3 million. For the first time since its launch three years ago, Sony Corp.'s PlayStation 3 sold more units than both the Nintendo Wii and the Microsoft Corp.'s Xbox 360.

"This portrays a very strong consumer reaction to the price decrease, as August and September both realized a lift of more than 70 percent over the prior month," said NPD analyst Anita Frazier of the PlayStation 3's performance.

Sony cut the price of the PlayStation 3 by $100 in August. Microsoft also slashed the Xbox 360's price by $100 that month, and Nintendo cut the Wii's price for the first time since its 2006 launch by $50 in late September. The average retail price of console hardware declined 8 percent from last September.

The top-selling gaming platform was still the handheld Nintendo DS, for the sixth month in a row.

Microsoft's "Halo 3: ODST" was by far the month's best-selling game. It helped push software sales 5 percent higher, to $649.3 million, though this was still well below what many analysts expected.

David Magee of SunTrust Robinson Humphrey forecast an increase in the low double digits. Wedbush Morgan's Michael Pachter expected a 21 percent jump.

Both "The Beatles: Rock Band" and "Guitar Hero 5" were among the top 10 best-selling games, along with Nintendo's "Wii Sports Resort" and "Madden NFL 10" for the Xbox 360.

Heavily Armed "Borderlands" Videogame Hits U.S.

"Borderlands," a videogame brimming with weaponry and battle, hit North America on Tuesday.

It takes aim at the rest of the world on Friday.

The title developed by Gearbox Software and published by 2K Games

combines one-on-one challenges, solo play, and online team options with a wasteland planet setting and lots of guns.

"Borderlands" contains automated weapon generating software that even served up surprises for its creators during a demonstration at a major E3 videogame conference in California earlier this year.

The videogame boasts "a near infinite variety" of weapons, and the overall objective for players is basically to find them and use them to annihilate enemies. The game's arsenal tops 17 million weapons, according to 2K.

"The 'Borderlands' team has brought together the things we know we love - co-op, skill-based action, character development and millions of guns - in a way we haven't seen before," said Gearbox president Randy Pitchford.

"I think it's the best video game we've ever made and I have never been more excited about a launch."

Borderlands allows players linked by the Internet to freely join or leave each others' games at any time for "collaborative mayhem" or solo adventure.

"Borderlands is unlike anything else on store shelves," said 2K president Christoph Hartmann. "It's got it all... and the biggest arsenal ever seen in a first-person shooter."

Versions of "Borderlands" tailored for play on Microsoft Xbox 360 and Sony PlayStation 3 consoles were released Tuesday in North America. The videogame software will be available in other markets beginning Friday.

Versions of the role-playing videogame for play on personal computers will be released next week.

The first downloadable expansion pack for "Borderlands" will star zombies; enemies dear to the hearts of shooter fans.

"The Zombie Island of Dr. Ned" for "Borderlands" is to be released by the end of the year.

Backyard Football '10 Charges into North American Retailers

Atari, one of the world's most recognized videogame publishers, announced Friday the release of "Backyard Football '10," the latest iteration of the number one youth football videogame franchise. Now available at retailers nationwide, and for the first time on the Xbox 360 video game and entertainment system from Microsoft, the title has earned Microsoft's "Family Games" status, which requires the game to pass a strict set of criteria based on rating, ease of play and audience appeal. Backyard Football '10 has also released on Wii and PlayStation2 computer entertainment system and features a star studded roster of NFL players featured as animated middle-schoolers in the game.

Packed with real football action,"Backyard Football '10" features all new co-op play for exciting 2 vs 2 action, enhanced controls, new unlockables, insane power ups, custom teams and characters, multiple play modes (single player, season play, tournament and all-pro) as well

as a hall of fame where kids can compare their season scores and rankings from Backyard Football ’09.

"Whether looking for a unique and realistic football experience or family friendly, easy gameplay environment to interact with your favorite NFL players, "Backyard Football ’10" is a title that will provide the best in youth gaming out there," said Keith Gordon, Vice President of Licensing, NFL PLAYERS. "We think fans of the franchise will be excited by the amount of impressive new features and look forward to watching as kids of all ages experience the thrilling gameplay "Backyard Football ’10" has to offer."

"The Backyard Football franchise continues to evolve, building on our past successes and adding exciting new features including co-op gameplay that allows kids and families to play together," said Jim Wilson, CEO, Atari, Inc. "We also look forward to continued success as we move this ’Family Friendly’ game onto the Xbox 360."

"Backyard Football ’10 "combines realistic NFL plays and strategies with wild arcade style power moves and comical scenarios so gamers of all ages can learn the fundamentals of football while having fun. Kid-friendly and non-violent, Backyard Football ’10 features multiple levels so it is easy for beginners to jump in a play, yet challenging enough for even die-hard football fans. The game lets kids customize their football players and teams, choose the season, style, location, pace, and strategy of the game and play a full season or single games.

"Backyard Football ’10" is rated "E" (for everyone) by ESRB and is available at retailers across North America for Xbox 360 ($39.99), Wii ($29.99) and PlayStation2 computer entertainment system ($19.99).

/Backyard Football is part of the /Backyard Sports series, the bestselling sport video game franchise for kids. Since 1996, the Backyard Sports franchise has sold nearly 12 million units and received over a hundred awards for excellent. What’s more, according to an independent study, 15 percent of boys in the United States, ages five to 10, own at least on Backyard Sports title.

=~=~=~=

A-ONE’s Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

Web Company CEOs Call for Net Neutrality Rules

Twenty-four top executives at e-commerce, social-networking and other Web companies have asked the U.S. Federal Communications Commission to move forward with its plan to create formal net neutrality rules, despite opposition voiced by several U.S. lawmakers, minority groups and telecom-related companies.

The Monday letter to the FCC, signed by the CEOs of Amazon.com, Google,

eBay, Facebook and Twitter, said net neutrality rules will ensure a "competitive and efficient" Internet marketplace.

Net neutrality rules prohibiting broadband providers from selectively blocking or slowing Web content and applications will allow an Internet "where consumers make the ultimate choices about which products succeed and which fail," the letter said. "This allows businesses of all sizes, from the smallest startup to larger corporations, to compete, yielding maximum economic growth and opportunity."

The FCC on Thursday is scheduled to vote on a process of formalizing some net neutrality principles that have been in effect at the agency since 2005. In September, FCC Chairman Julius Genachowski called on the commission to create formal regulations.

The new letter, organized by pro-net neutrality group the Open Internet Coalition, comes as several other groups have expressed concerns about net neutrality regulations. In the past week, 90 U.S. lawmakers have signed onto two letters to the FCC, both questioning whether new rules would dampen investment in broadband networks. One of the letters was signed by 72 Democratic lawmakers, even though Democrats have traditionally supported calls for new net neutrality rules.

The FCC should "carefully consider the full range of consequences that government action may have on network investment," the Democratic letter said. "In light of the growth and innovation in new applications that the current [regulatory] regime has enabled, as compared to the limited evidence demonstrating any tangible harm, we would urge you to avoid tentative conclusions which favor government regulation."

In addition, 44 telecom-related companies, including Cisco Systems, Alcatel-Lucent, Ericsson and Nokia, have questioned the need for net neutrality rules, and a coalition of minority groups, including the Hispanic Technology and Telecommunications Partnership, the National Association for the Advancement of Colored People (NAACP), the Asian American Justice Center, have questioned whether net neutrality rules would slow the deployment of broadband to areas with large minority populations.

But the 24 Internet executives argued in their letter that for most of the Internet’s history, traditional telecom companies lived with rules that required them to share their networks and carry all traffic. The FCC in 2005 ended network-sharing rules for telecom carriers.

"Entrepreneurs, technologists, and venture capitalists have previously been able to develop new online products and services with the guarantee of neutral, nondiscriminatory access by users, which has fueled an unprecedented era of economic growth and creativity," the letter said. "Existing businesses have been able to leverage the power of the Internet to develop innovative product lines, reach new consumers, and create new ways of doing business."

Several of the companies signing the Monday letter have already expressed support for net neutrality rules.

Among those signing the letter were Craig Newmark, founder of Craigslist; Caterina Fake, founder of Flickr; Stan Glasgow, president and chief operating officer of Sony Electronics; and John Lilly, CEO of Mozilla.

Fake Security Software in Millions of Computers

Tens of millions of U.S. computers are loaded with scam security software that their owners may have paid for but which only makes the machines more vulnerable, according to a new Symantec report on cybercrime.

Cyberthieves are increasingly planting fake security alerts that pop up when computer users access a legitimate website. The "alert" warns them of a virus and offers security software, sometimes for free and sometimes for a fee.

"Lots of times, in fact they're a conduit for attackers to take over your machine," said Vincent Weafer, Symantec's vice president for security response.

"They'll take your credit card information, any personal information you've entered there and they've got your machine," he said, referring to some rogue software's ability to rope a users' machine into a botnet, a network of machines taken over to send spam or worse.

Symantec found 250 varieties of scam security software with legitimate sounding names like Antivirus 2010 and SpywareGuard 2008, and about 43 million attempted downloads in one year but did not know how many of the attempted downloads succeeded, said Weafer.

"In terms of the number of people who potentially have this in their machines, it's tens of millions," Weafer said.

It was also impossible to tell how much cyberthieves made off with but "affiliates" acting as middlemen to convince people to download the software were believed to earn between 1 cent per download and 55 cents.

TrafficConverter.biz, which has been shut down, had boasted that its top affiliates earned as much as $332,000 a month for selling scam security software, according to Weafer.

"What surprised us was how much these guys had tied into the whole affiliated model," Weafer said. "It was more refined than we anticipated."

Experts See Forecast Worsen for Cybercrime

Law enforcement agencies can count a few recent victories against cybercriminals, but agents say the battle against them isn't getting any easier.

Highly organized cybercriminals are using increasingly sophisticated tools and methods that make them hard to trace, said Keith Mularski, supervisory special agent with the U.S. Federal Bureau of Investigation's Cyber Division.

"They have evolved over the years," Mularkski said. "It really is organized crime."

Mularski, who spoke at the RSA conference in London on Wednesday, has had great success in infiltrating organized cybercrime rings. He successfully infiltrated a ring known as DarkMarket, an online forum where criminals bought and sold personal data, such as credit card numbers. DarkMarket was shut down about a year ago and 59 people were arrested, with the help of authorities in the U.K., Germany, Turkey and other countries.

While the DarkMarket bust was a big win, there are still such forums operating today and they're hard to infiltrate. New members must be vetted for reliability and to ensure they're not agents like Mularski.

The malicious software programs used to collect the data have become insidiously complicated and hard to detect. Financial organizations now are in a "raging battle" against "high-grade" weaponry, said Uri Rivner, RSA's head of new technologies for identity protection and verification, who gave a presentation earlier in the day at RSA.

Those programs go by names such as Sinowal - also known as Mebroot and Torpig - which is a nasty rootkit that burrows in a computer's master boot record below the OS. It may not even be removed by reinstalling the operating system. It can steal data and even modify the HTML of Web pages requested by a user.

Computers that do not have up-to-date software patches are in particular danger. Hackers often set up Web sites or hack legitimate ones to perform what's called a "drive-by" download, which automatically exploits vulnerable software programs to infect a computer.

Microsoft has particular insight into the problem. Late last month, the company released its free Security Essentials antivirus software and so far it has been downloaded 3.5 million times, said Amy Barzdukas, Microsoft's general manager for Internet Explorer and Consumer Security, who also spoke at RSA.

More than 30 percent of those computers running Security Essentials needed "a fair amount of cleaning of viruses, Trojans and rootkits," she said.

While it may be hard for law enforcement to figure out who is writing those malicious programs, they do have a clear five-prong strategy for how to disrupt the cybercrime operations.

Agents try to infiltrate the groups if possible, said Andy Auld head of intelligence of the e-crime department for the U.K.'s Serious Organized Crime Agency, who spoke alongside Mularski.

Following the money exchanged for personal data is also a "critical path," Auld said. Tracking down stolen data is important, as credit card numbers that are being traded can be shut down before the criminals have a chance to use or sell the numbers.

Another path is finding ways to revoke the IP (Internet Protocol) address allocations given to cybercriminals running servers. Those allocations are given by five organizations, including the RIPE Network Coordination Center, he said.

The FBI has become more proactive in dealing with fast-breaking cybercrime issues, Mularski said. For example, the FBI has issued public service advisories warning people of online-related hazards, stepping

away from its secretive tradition.

"We're adapting," Mularski said. "We're making great strides."

FDA Warns: Swine Flu Scams Lurk on the Internet

Air "sterilizers." A photon machine. Supplement pills to boost the immune system. Protective shampoos and face masks. Even fake Tamiflu.

These and other products making bogus claims to prevent or treat swine flu are flooding the Internet as scam artists prey on the public's fears while the vaccine is delayed and real Tamiflu - made by Switzerland's Roche Group - is rationed.

Every problem, it would seem, is a sales opportunity. Some of the products appear to have been pitched for other emergencies, such as one called "Quake Kare" and masks and purifiers sold during the SARS scare.

Federal officials have sent warning letters to promoters of more than 140 swine flu-related products, including well-known alternative medicine advocate Dr. Andrew Weil for his "Immune Support Formula."

Consumer Reports also has warned subscribers to be wary.

"It's harmful, disappointing, frustrating to see folks take advantage of the public like this," said Dr. John Santa, who evaluates health claims for Consumer Reports.

Fraudulent products emerged shortly after swine flu did last spring - about 10 a day, said Alyson Saben, head of a swine flu consumer fraud team formed by the Food and Drug Administration. The pace slowed over the summer as the flu abated, but "it's picked up" in recent weeks, she said. "We are seeing new sites pop up."

Most worrisome: sites that claim to sell Tamiflu without a prescription. The FDA bought and tested five such products. One contained powdered talc and generic Tylenol - no Tamiflu. Several others contained some Tamiflu but were not approved for sale in the U.S.

"We have no idea of the conditions under which they were manufactured. They could contain contaminated, counterfeit, impure or subpotent or superpotent ingredients," Saben said.

Tamiflu and GlaxoSmithKline's Relenza are the only drugs recommended for treating swine flu.

Rogue Web sites are not the only ones trying to cash in on flu fears. Makers of some well-established products are making claims that may be close to the line, the FDA says.

This week, the makers of Dial Soap, Kleenex, Clorox and other big brands launched a joint promotional campaign costing up to $1 million. The FDA is reviewing the campaign, which includes a video that says:

"Germs are tiny organisms that can cause disease. According to the CDC, up to 80 percent of infectious diseases, like the flu, are spread by your hands. That's why frequent, proper handwashing is so important in

preventing spread of the flu, other viruses and germs. An antibacterial soap like Dial Complete foaming hand wash kills 99.9 percent of germs."

Flu is caused by a virus, so killing bacteria is of uncertain benefit.

The campaign is "not being specific down to swine flu," said Scott Moffitt, an official with Dial Corp.'s parent company, Germany-based Henkel AG. He also contends the video is not misleading, even though the germ-killing claim follows a sentence about flu and other viruses.

One product that drew a warning letter from the FDA is the Photon Genie, a gadget that delivers "energy waves." Its Web site claimed it "helps strengthen the immune system, and a strong immune system is KEY to preventing swine flu symptoms and KEY to treating swine flu."

The site has since removed the swine flu claim but "other claims remain," Saben said.

The group behind the Web site, the Skilling Institute of Phoenix, "is not marketing, and will not market in the future, any product that is intended to diagnose, mitigate, prevent, treat or cure the H1N1 flu virus," its director, Warren Starnes, wrote in an e-mail.

Some products the FDA warned about contain silver, such as "Swine Flu...Gone," made by Secrets of Eden.

"Spray 'Swine Flu...Gone' with ionic silver on your hands and on any surface where these germs may exist and kill the virus," its site had claimed.

Secrets of Eden sells supplements and oils with a biblical flair, said its general manager, Rick Strawcutter, a former pastor in Adrian, Mich. The staff "got a little carried away" on marketing for one product and "drew the ire of the FDA," he said.

"It was not worth contesting," so he ordered a stop to it, Strawcutter said.

The federal Agency for Toxic Substances and Disease Registry says silver "may cause harmful health effects," depending on the amount and type of exposure.

Dr. Andrew Weil's site had this problem language, the FDA's warning letter said: "...during the flu season, I suggest taking a daily antioxidant, multivitamin-mineral supplement, as well as astragalus, a well-known immune-boosting herb that can help ward off colds and flu. You might also consider ... the Weil Immune Support Formula which contains both astragalus and immune-supportive polypore mushrooms."

Weil issued a statement saying the content "was primarily educational" about how to avoid the flu, and that he had directed his Web site team to remove and review it for compliance with federal rules.

Doctors, too, are being warned not to prescribe unproven remedies, such as drugs not shown to be safe and effective for swine flu. In this week's New England Journal of Medicine, three FDA doctors caution against use of ribavirin, a drug approved in the U.S. for treating hepatitis C and respiratory syncytial virus, or RSV, a childhood illness.

There have been reports of doctors wanting to try it for seriously ill

flu patients, but it can cause a dangerous type of anemia and cannot be used in pregnant women because of the risk of birth defects, said the FDA’s Dr. Debra Birnkrant.

"It shouldn’t be used lightly" and needs to be tested in a clinical trial for flu, she said.

Nigeria, Software Firms Look To Halt Internet Crime

Nigeria’s anti-corruption police is working with top computer software companies to halt thousands of fraudulent emails in a crackdown on internet crime in Africa’s most populous country, an agency spokesman said.

The Economic and Financial Crimes Commission (EFCC) said on Thursday its new project "Eagle Claw," expected to become fully operational within six months, aimed to improve Nigeria’s tarnished image as one of the world’s top countries for internet crime.

"The EFCC is fine tuning security modalities with Microsoft, and upon full deployment, the capacity to take down fraudulent emails will increase to 5,000 monthly," said Farida Waziri, the agency’s chairwoman, in a statement.

The government said it would also be working with Yahoo and Google to monitor online traffic to block millions of email spam coming from Nigeria.

"The technology is not yet fully developed, but operatives will be working on 24 hours, 7 days a week to detect key words found in fraudulent emails. Only clean email can go out," said EFCC spokesman Femi Babafemi.

The agency said it has already shut down 800 scam websites and arrested 18 people in the last three months. It will have at least 100 EFCC officials dedicated to the project.

The initiative is the latest effort by the government to shrug off its image as an epicenter of corruption, epitomized by "419" email fraudsters named after the article in Nigeria’s penal code that deals with advance fee fraud.

The government last month banned the showing of blockbuster sci-fi movie "District 9," which caricatures Nigerians as gangsters and cannibals, and demanded an apology from Sony after a Playstation advert implied they are fraudsters.

President Umaru Yar’Adua has also launched a rebranding campaign with the slogan: "Nigeria: Good People, Great Nation," and started a nationwide initiative to promote "Made In Nigeria" products over foreign imports.

But Nigerians, most of whom live on less than $2 a day, say the government needs to do more to address the everyday problems of the oil-rich, but impoverished country.

Phishers Dangle Some Brand-New Bait

In September 2009, some unlucky visitors at the New York Times Web site clicked on an ad that attempted to install malware. The advertisement displayed a popup window informing readers that their computer might be infected with a virus; only by purchasing a new antivirus product could they be sure of having a clean system.

The Times later acknowledged the scam in a posting on its Web site: "Some NYTimes.com readers have seen a pop-up box warning them about a virus and directing them to a site that claims to offer antivirus software....If you see such a warning, we suggest that you not click on it. Instead, quit and restart your Web browser." Phishers and scammers use this and other new tactics to deceive unsuspecting victims.

Phishing refers to an attempt to collect usernames, passwords, and credit card data by posing as a legitimate, trusted party. Often the deception involves using e-mail sent from a trusted address. Originally, /phishing/ applied to the banking and payment industry only, but now it also covers theft of log-in credentials to games, and personal passwords to social networks such as Facebook and Twitter.

Most people wouldn’t reveal their social security number or mother’s maiden name at a strange site. Modern browsers and security software flag such content and ask you whether you’re sure you want to send it; some block it with a red-and-black warning label. So phishers have adopted new tactics.

Rogue antivirus products are among the latest phishing instruments to appear, and many are quite convincing. Bearing names like Antivirus 2009, AntiVirmin 2009, and AntiSpyware 2009, they have interfaces similar to those of real antivirus apps. Some rogue antivirus products have their own keywords on search engines and cite fake reviews recommending them (including one that I supposedly wrote.

The rogue antivirus product that showed up on the New York Times site installed malware that, if executed, would have lowered the security settings in Internet Explorer, run executable files, and altered the system Registry. Such actions by phishing malware are fairly common. The real security apps knew it, too: Legitimate antivirus vendors AVG, Comodo, Kaspersky, McAfee, Microsoft, Nod32, and Sophos, (among others) detected this particular piece of malware within the first few hours.

Another phishing gambit is a variation on an old scam: The crooks mass-mail a seemingly personalized e-mail message, ostensibly from a bank, containing a fake online chat option.

In this "chat-in-the-middle" attack, as soon as the victim enters a user name and password at the designated online site, a chat window opens up and a scammer posing as a customer service rep at the bank requests additional personal information to confirm the identity of the account holder. By providing these details, the victim gives the thief crucial data.

Roger Thompson, chief research officer at AVG, says rogue antivirus products are common: "The bad guys are clearly making money at it." Besides benefiting up front by selling the rogue antivirus product, they collect credit card information for future identity fraud.

Jon Miller, director of Accuvant Labs, a security consulting firm that works with Fortune 500 companies and several U.S. government contractors, says that the New York Times incident isn't unusual. Further, he notes that he has seen an upsurge in the use of malware tailored to customers of particular banks and other financial institutions.

AVG makes a free product called LinkScanner that blocks new phishing attacks, yet allows users to safely view any site. For phishing attacks such as fake chat sessions and fake keywords, AVG's Thompson says, users need to develop a healthy dose of skepticism, and learn how to kill the browser using Task Manager. That won't stop Web-based exploits, but it will give you a way to defeat social engineering attacks.

Accuvant's Miller recommends several common-sense antiphishing strategies:

* Use a strong browser. According to Miller, Internet Explorer is the weakest browser, while Firefox and Google Chrome are relatively strong.
* Use a malware-resistant platform such as Mac OS or Linux. Though neither is impervious to attack, each is less likely to be targeted than the mainstream Windows operating system.
* Use antimalware software; Miller says that his program of choice is Webroot Internet Security Essentials.
* Update your software promptly and regularly, but don't depend on updates as the sole way to guarantee your system's security. As Miller observes, "malware tends to be ahead of the curve."
* Be cautious and vigilant when using high-profile social networking sites such as Facebook and Twitter.

U.S. Man to Serve Prison Term for Selling Counterfeit Software

A 46-year-old Falls Church, Virginia, man has been sentenced to 41 months in prison for selling counterfeit software on eBay, the U.S. Department of Justice said.

Gregory William Fair was sentenced Thursday in U.S. District Court for the District of Columbia. In addition to the prison term, Judge R.W. Roberts ordered Fair to pay US$743,098 in restitution.

Fair has forfeited $144,000 seized from a safety deposit box and residence, one BMW 525i, one Hummer H2, one Mercedes CL600 and one 1969 Pontiac GTO. All the cars were purchased using funds from his counterfeit software operation, the DOJ said.

Fair pleaded guilty on April 16 to one count of criminal copyright infringement and one count of mail fraud for selling pirated business software. The software Fair sold between 2001 and 2007 had a combined retail value of more than $1 million, the DOJ said.

During his plea, Fair said he used a variety of eBay user IDs to sell counterfeit software.

The case is part of the DOJ's ongoing initiative to combat the sale of pirated software and counterfeit goods through commercial Web sites and online auction sites. The DOJ has obtained 39 convictions involving online auction and commercial distribution of counterfeit software.

Ballmer Launches ’Simpler, Faster’ Windows 7

Microsoft chief executive Steve Ballmer officially unveiled the company’s new Windows 7 operating system at a Thursday launch event in Manhattan.

"I’m Steve Ballmer and I’m a Windows 7 PC," he announced.

The idea behind the new OS is to make computing "simpler, faster, more responsive," he said. That was possible thanks to an "intense collaboration" between Microsoft and its partners - 50,000 software, hardware, and peripheral vendors, as well as 8 million beta testers, he said.

"Windows needs to be an incredible opportunity for innovation, for hardware companies [and] software companies, and it needs to be a place that is simple and easy to use and opens up the world of diverse innovation - in a way that is manageable and consumable by billions of people around the world," Ballmer said.

Ballmer pointed to three key components of the OS: it works in the way you want it to work, it simplifies, and it enables new technologies.

Users want their PC to fire up quickly, to be responsive, and have a longer battery life, and "I think we’ve accomplished that" with Windows 7, Ballmer said.

"The things that you do all the time need to be simpler," Ballmer said. "You want to manage the windows on your desktop [and] make that stuff super, super simple."

New technologies include the OSes multi-touch computing capabilities, he said.

"Frankly, there’s more you can do with this system," Ballmer said. "Ninety-five times out of 100, if people have a choice, they choose a PC."

Microsoft announced that next month, Amazon will launch a beta version of the Kindle Reader for Windows 7, which will allow users to peruse books using multi-touch. Scroll through a book with the touch of a finger, and zoom in or out by pinching the screen.

"From the end-user perspective, you get dozens or hundreds of new features - everybody finds their own unique set of features to fall in love with," he said.

Ballmer was introduced by Kylie, the precocious five-year-old who is the star of Microsoft’s latest ad campaign. "You were late," she informed him when Ballmer asked if she had enjoyed their meeting yesterday. He blamed airport delays and then presented her with a pink netbook as a consolation prize.

Long Lines As Microsoft Opens Retail Store

The idea that hundreds of people would line up outside anything to do with Microsoft would have been far-fetched only a few years ago - but on Thursday that’s what happened when the software giant opened its first retail store in Scottsdale, Arizona.

Around 500 people, some of whom had camped out all night, waited in line for the opening of store the Fashion Square Mall in this upscale city, where they were met with cheers by staff wearing Microsoft T-shirts.

Microsoft has at least partially succeeded in changing opinion about its lack of coolness, helped by positive reviews for its new Windows 7 operating system.

"It’s a good idea to give consumers a warm and fuzzy (feeling) about using an operating system... It will make consumers feel better about their purchase," said shopper Hafthor Stefansson, an IT consultant who said he uses both Apple and Microsoft systems, as he stood outside the store.

The Scottsdale store is the first of a planned chain of Microsoft-branded stores, aiming to match rival Apple Inc’s successful foray into retailing.

It is Microsoft’s second bite at the retail business after a short-lived experiment in conjunction with Sony Corp in San Francisco’s Metreon Center 10 years ago.

Customers picked over hardware including Xbox 360s, Hewlett-Packard Co and Dell Inc laptops, as well as the Windows 7 operating system, which launched on Thursday.

Microsoft said in February it planned to open stores, hiring a former Wal-Mart Stores Inc executive to run them. A second store is due to open shortly in Orange County, California.

Microsoft may have a way to shed its traditionally dowdy image and emulate Apple’s splashy store openings and product launches. For example, when Apple began selling its 3G iPhone in July 2008, thousands of people from all over the world camped outside its stores for days for the chance to buy one.

Microsoft Chief Executive Steve Ballmer said last week that through the stores, the company was looking to make a direct connection with users, showing the "customer what you really can do".

"They’re doing exactly what Apple did five years ago - the concept’s a rip off," said James Smith, 31, a taxi driver who turned out for the opening. "Microsoft might have come up with a better idea than taking Apple’s straight out."

But videographer Erin Phoenix, a long-time Apple user wearing an iPhone T-shirt to the opener, said he thought the result would be good for consumers.

"They are kind of copying the concept the Apple Stores have of customer service ... (but) it will also give Apple more competition."

At the nearest Apple Store, several miles away in Phoenix, a few dozen customers browsed computers and applications.

"I’m Microsoft free... so it’s not of interest," said Jerry Delgado, an IT specialist who sells professional audio and video equipment.

"I’m not a Windows user, I’m not an Office user, so they really don’t offer anything else that I would buy... I’m satisfied with Apple."

Alyssa Shevlin, who had bought a PowerBook and iPod, also was uninterested in the Microsoft store.

"My computer is compatible with my iPod, so I see no need to go over there."

Apple Unveils New Macs for The Holidays

Apple Inc rolled out a new line of redesigned Mac computers on Tuesday, hoping to build up sales momentum for its biggest business heading into the all-important holiday season.

Sporting new features such as touch-based mice and edge-to- edge glass, Apple hopes to sustain the fast-growing sales of its computers. Allaying initial worries about its premium pricing, Apple’s Mac business has been surging despite a recession that has pinched consumer spending.

Mac unit sales - the largest single contributor to Apple’s revenue - leaped 17 percent in the quarter, far outpacing the PC market. That helped Apple blow by Wall Street forecasts on quarterly earnings and revenue. Its shares rose 5 percent to $198.99 in afternoon trading on the Nasdaq.

Chief Operating Officer Tim Cook told Reuters in an interview the company was packing more features and functions into its new iMac, MacBook and Mac Mini computers.

"You can just see that it’s working with the results that we’ve had," he said. "We’re not interested in the netbook phenomenon of cheap and crappy and people that want to return it after a day or two. That’s just not who we are."

With average selling prices coming down across the PC industry as PC makers from Dell Inc to Hewlett-Packard Co vie for consumers’ shrinking spending, some analysts had said Apple might face renewed pressure to cut prices.

It kept entry prices the same on its new Macs, although prices on higher-end configurations came down.

The most significant change came in Apple’s line of iMac all-in-one desktop computers, which now feature a new edge-to-edge glass design and aluminum enclosure. The iMac starts at $1,199.

The iMac will ship with Apple’s new "Magic Mouse," which features multi-touch technology such as found on the iPhone. It has no mechanical buttons, balls or scroll wheels and users can navigate using finger gestures.

New MacBook laptops are lighter at 4.7 pounds. Cook said some features from the more expensive MacBook Pro line, such as the unibody design,

will now be found on the MacBook, which starts at $999.

Laptops sales leaped 35 percent last quarter and represented nearly three-quarters of the Mac sales mix.

"The key is driving that notebook adoption," said Broadpoint Amtech analyst Brian Marshall.

He said it was difficult to get worried about Mac prices after the performance Apple turned in on Monday.

The Mac mini, Apple's lowest-priced computer at $599, was also updated, with more speed, storage and memory.

"This finalizes our lineup for the holiday season," Cook said. "I feel great about our position going into it."

Snow Leopard Purring on a PC?

When is a Windows PC not a Windows PC? When you toss out the Windows and replace it with Apple's Mac OS X Snow Leopard or any other major operating system.

That's what you can do - at least for the moment - with Rebel EFI from Psystar Corp., a $50 application suite that allows standard PC boxes with Intel Core 2 Duo, Core 2 Quad, Core i7 or Xeon Nehalem processors to install and run multiple operating systems. This capability had been built into Psystar's computers in the past, but now the software that enables it is available as a standalone, user-installable product.

The road isn't clear for Rebel EFI, however, as Psystar is embroiled in an ongoing legal tussle with Apple over Psystar's virtualization technology. Until a court rules otherwise, however, you can download a free demo version of the Rebel EFI suite, limited to two hours of run time, from Psystar's Web site so you can be sure that the software will work with your hardware.

Once the download is burned to a CD, you can boot your PC with Rebel EFI and then proceed to install Mac OS X Snow Leopard or any other major operating system using standard installation discs. Rebel EFI scans the connected hardware and automatically downloads and installs any necessary drivers, according to Psystar.

Psystar's Darwin Universal Boot Loader, included with Rebel EFI, is the core utility which allows PC hardware to load multiple operating systems, including Windows 7, Mac OS X and the various iterations of Linux. The demo version can be upgraded to the full version by purchasing a registration code. Psystar also announced a new Psystar Labs approval initiative under which users having trouble with Rebel EFI and their computer hardware can have the devices analyzed and, if a solution is found, certified by the company.

Minnesota Man Suspected of Encouraging Suicides

A nurse who authorities say got his kicks by visiting Internet suicide chat rooms and encouraging depressed people to kill themselves is under investigation in at least two deaths and could face criminal charges that could test the limits of the First Amendment.

Investigators said William Melchert-Dinkel, 47, feigned compassion for those he chatted with, while offering step-by-step instructions on how to take their lives.

"Most importatn is the placement of the noose on the neck ... Knot behind the left ear and rope across the carotid is very important for instant unconciousness and death," he allegedly wrote in one Web chat.

He is under investigation in the suicides of Mark Drybrough, 32, who hanged himself at his home in Coventry, England, in 2005, and Nadia Kajouji, an 18-year-old from Brampton, Ontario, who drowned in a river in Ottawa, where she was studying at Carleton University.

While the victims' families are frustrated that no charges have been filed, legal experts said prosecuting such a case would be difficult because Melchert-Dinkel didn't physically help kill them. In the meantime, he has been stripped of his nursing license.

"Nothing is going to come of it," Melchert-Dinkel said of the allegations during a brief interview with The Associated Press. "I've moved on with my life, and that's it."

The case came to the attention of Minnesota authorities in March 2008 when an anti-suicide activist in Britain alerted them that someone in the state was using the Internet to manipulate people into killing themselves.

Last May, a Minnesota task force on Internet crimes searched Melchert-Dinkel's computer and found a Web chat between him and the young Canadian woman describing the best way to tie knots. In their search warrant, investigators said Melchert-Dinkel "admitted he has asked persons to watch their suicide via webcam but has not done so."

Authorities said he used such online aliases as "Li Dao," "Cami" and "Falcon Girl."

The Minnesota Board of Nursing, which revoked his license in June, said he encouraged numerous people to commit suicide and told at least one person that his job as a nurse made him an expert on the most effective way to do it.

The report also said Melchert-Dinkel checked himself into a hospital in January. A nurse's assessment said he had a "suicide fetish" and had formed suicide pacts online that he didn't intend to carry out.

In excerpts of a Web chat between Kajouji and Melchert-Dinkel, provided by Kajouji's mother, he allegedly gave the young woman both emotional support and technical advice on hanging.

"im just tryin to help you do what is best for you not me," one message said, posted using the alias "Cami." Kajouji's mother said she was given a transcript by Ottawa police.

In another exchange, "Cami" tried to persuade Kajouji to hang herself instead of jumping into a freezing river: "if you wanted to do hanging

we could have done it together on line so it would not have been so scary for you"

Melchert-Dinkel, who lives in Faribault, about 45 miles from Minneapolis, worked at various hospitals and nursing homes over the years and was cited several times for neglect and being rough with patients, according to the nursing board.

Task force spokesman Paul Schnell would not say when or if charges would be filed and stressed that the investigation is complicated because of the anonymity of Web chat rooms. He said the task force is also looking into whether Melchert-Dinkel was involved in other suicides.

In obtaining the search warrant for Melchert-Dinkel's computer, Minnesota authorities cited a decades-old, rarely used state law that makes it a crime to encourage someone to commit suicide. The offense carries up to 15 years in prison.

The law does not specifically address situations involving the Internet or suicides that occur out of state.

George Washington University Law School professor Jonathan Turley, who follows the issue of physician-assisted suicide, said he has never heard of anyone being prosecuted for encouraging a suicide over the Internet.

Typically, people are prosecuted only if they physically help someone end it all - for example, by giving the victim a gun, a noose or drugs. Last month, a Florida man was charged in his wife's suicide after allegedly tossing several loaded guns onto their bed.

Turley said if prosecutors file charges against Melchert-Dinkel, convicting him will be difficult - especially if the defense claims freedom of speech.

The law professor said efforts to make it illegal to shout "Jump!" to someone on a bridge have not survived constitutional challenges. "What's the difference between calling for someone to jump off a bridge and e-mailing the same exhortation?" he said.

But Kajouji's mother, Deborah Chevalier, said in an e-mail: "He is a predator who is responsible for several deaths and needs to be held legally accountable for them."

Judge Dismisses 'Adult Services' Craigslist Suit

A federal judge has thrown out a lawsuit aimed at driving classified ads for prostitution off the Craigslist Web site.

U.S. District Court Judge John Grady said not all postings on the Craigslist "Adult Services" section advertised prostitution and that other services could legitimately appear there.

"A woman advertising erotic dancing for male clients is offering an adult service, yet this is not prostitution," he said in a 31-page opinion Tuesday.

He said such an ad "might even be entitled to some limited protection

under the First Amendment" to the U.S. Constitution.

Grady also said Craigslist is not to blame if those who post ads violate the San Francisco-based Web site's guideline barring prostitution ads.

Cook County Sheriff Tom Dart filed the lawsuit against Craigslist in July, saying a change in the category name from "Erotic Services" to "Adult Services" had failed to deter prostitutes from using the site.

"Sheriff Dart may continue to use Craigslist's Web site to identify and pursue individuals who post allegedly unlawful content," Grady said. "But he cannot sue Craigslist for their conduct."

Dart said in a telephone interview that the sheriff's department has made hundreds of prostitution arrests related to Craigslist in the last two years. He said his investigators scan the list for names and phone numbers, arrange to meet prostitutes at hotels and arrest them when they offer sex for money.

"It isn't that I just woke up one morning and said, 'Let's sue Craigslist,'" Dart said. "This came after two years and hundreds of arrests off of the Web site, and many of the arrests involve juveniles and human trafficking."

He said he was still deciding whether to appeal.

Responding to the ruling, Craigslist CEO Jim Buckmaster said through a spokeswoman: "We welcome Judge Grady's decision on this matter."

Dart and other critics acknowledge that when Craigslist pulled the plug on its "Erotic Services" category a number of pictures of scantily clad women in suggestive poses disappeared from the Web site.

But Dart says its plain that prostitution is still being advertised.

Report Says China Ready for Cyber-war, Espionage

Looking to gain the upper hand in any future cyber conflicts, China is probably spying on U.S. companies and government, according to a report commissioned by a Congressional advisory panel monitoring the security implications of trade with China.

The report outlines the state of China's hacking and cyber warfare capabilities, concluding that "China is likely using its maturing computer network exploitation capability to support intelligence collection against the U.S. government and industry by conducting a long term, sophisticated computer network exploitation campaign." Published Thursday, the report was written by Northrop Grumman analysts commissioned by the US-China Economic and Security Review Commission.

Government agencies and military contractors have been hit with targeted, well-crafted attacks for years now, many of which appear to have originated in China. But this report describes in detail how many of these attacks play out, including an attack that exploited an unpatched flaw in Adobe Acrobat that was patched earlier this year.

Citing U.S. Air Force data from 2007, the report says at least 10 to 20

terabytes of sensitive data has been siphoned from U.S. government networks as part of a "long term, persistent campaign to collect sensitive but unclassified information." Some of this information is used to create very targeted and credible phishing messages that then lead to the compromise of even more computers.

Northrop Grumman based its assessment largely on publicly available documents, but also on information collected by the company's information security consulting business.

The report describes sophisticated, methodical techniques, and speculates on possible connections between Chinese government agencies and the country's hacker community, increasingly a source of previously unknown "zero-day" computer attacks.

"Little evidence exists in open sources to establish firm ties between the [People's Liberation Army] and China's hacker community, however, research did uncover limited cases of apparent collaboration between more elite individual hackers and the [People's Republic of China's] civilian security services," the report says.

If true, that wouldn't be much of a surprise. The U.S. government has had a presence at the Defcon hacker convention for years now, and the U.S. Department of Defense has even started using it as a recruitment vehicle in recent years.

The Adobe Acrobat attack was supplied by black hat programmers to attackers who targeted an unnamed U.S. firm in early 2009. Working nonstop in shifts, the attackers snooped around the network until an operator error caused their rootkit software to crash, locking them out of the system.

In a typical targeted attack, the victim receives an email message containing a maliciously crafted office document as an attachment. It might be disguised to look like the schedule or registration form for an upcoming conference, for example. When it's opened, the zero-day attack executes and cyberthieves start collecting information that might be used in future campaigns. They sniff network and security settings, look for passwords, and even alter virtual private network software so they can get back into the network. In some cases they've installed encrypted rootkits to cover their tracks, or set up staging points to obscure the fact that data is being moved off the network.

In another case cited by Northrop Grumman, the attackers clearly had a predefined list of what they would and would not take, suggesting that they had already performed reconnaissance on the network. "The attackers selected the data for exfiltration with great care," the report states. "These types of operational techniques are not characteristic of amateur hackers."

Earlier this year, Canadian researchers described a similarly sophisticated cyberespionage network, called GhostNet, launched against international government agencies and pro-Tibetan groups such as the Office of His Holiness the Dalai Lama.

Although the GhostNet report authors did not link the spying to the Chinese government, some researchers did.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.